HB

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Takeshi INADA

Serial No. (unknown)

Filed herewith

ENCRYPTION-DECRYPTION APPARATUS

CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119 AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan on April 19,2000, under 2000-118269.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel

Benoît Castel
Attorney for Applicant
Customer No. 000466
Registration No. 35,041
745 South 23rd Street
Arlington, VA 22202
703/521-2297

April 18, 2001

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ４月１９日

出 願 番 号
Application Number: 特願２０００－１１８２６９

出 願 人
Applicant (s): 日本電気通信システム株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ２月１６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

【書類名】　特許願

【整理番号】　01612076

【あて先】　特許庁長官殿

【国際特許分類】　G09C

G06F

H03M

H04L

【発明者】

【住所又は居所】　東京都港区三田一丁目４番２８号

日本電気通信システム株式会社内

【氏名】　稲田　剛

【特許出願人】

【識別番号】　000232254

【氏名又は名称】　日本電気通信システム株式会社

【代理人】

【識別番号】　100082935

【弁理士】

【氏名又は名称】　京本　直樹

【電話番号】　03-3454-1111

【選任した代理人】

【識別番号】　100082924

【弁理士】

【氏名又は名称】　福田　修一

【電話番号】　03-3454-1111

【選任した代理人】

【識別番号】　100085268

【弁理士】

【氏名又は名称】　河合　信明

【電話番号】　03-3454-1111

【手数料の表示】

【予納台帳番号】　021566

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9114193

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号復号化装置

【特許請求の範囲】

【請求項１】　データの暗号化と暗号化データの複合化を行う暗号復号化装置において、暗号化復号化する回路を可変可能な回路装置を用い、前記可変可能な回路装置の回路データを秘密鍵として暗号化複合化を行うことを特徴とする暗号復号化装置。

【請求項２】　前記可変可能な回路装置の回路データを複数個有し、暗号化複合化を行うための回路データ選択情報から、前記可変可能な回路装置の回路データを選択し供給することで異なるアルゴリズムの暗号化複合化を行うことを特徴とする請求項１記載の暗号化復号化装置。

【請求項３】　入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきて前記暗号化データを入力し、暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は暗号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ＲＯＭ）とを有し、前記受信装置は復号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ＲＯＭ）とを有していることを特徴とする暗号復号化装置。

【請求項４】　入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記書き換え情報の指示に従い前記複数のＲＯＭを選択し、選択したＲＯＭか

ら暗号化する回路データを送出するセレクターと；

どのＲＯＭを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワーク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを、暗号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記書き換え情報の指示に従い前記複数のＲＯＭを選択し、選択したＲＯＭから復号化する回路データを送出するセレクターと；

どのＲＯＭを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記暗号化データを、復号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有することを特徴とする暗号復号化装置。

【請求項５】　入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、解析データを出力する

データ解析部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成を変更する第１の回路データを入力し、第２の回路データを生成出力するフィールド・プログラマブル・ゲートアレイ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ：以下ＦＰＧＡと記す）回路データ生成部と；

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号化する前記第１の回路データを前記ＦＰＧＡ回路データ生成部に出力するセレクターと；

前記ＦＰＧＡ回路データ生成部が出力する前記第２の回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワーク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、解析データを出力するデータ解析部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成を変更する第１の回路データを入力し、第２の回路データを生成出力するＦＰＧＡ回路データ生成部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号を復号化する前記第１の回路データを前記ＦＰＧＡ回路データ生成部に出力するセレクターと；

前記ＦＰＧＡ回路データ生成部が出力する前記第２の回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了

すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有することを特徴とする暗号復号化装置。

【請求項６】　前記送信装置が、

前記入力データを入力保持し、終了通知信号を受けると保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュＲＯＭと；

前記入力データを入力し、第１の回路データを前記フラッシュＲＯＭに出力し、この第１の回路データによりフラッシュＲＯＭのデータを書き換え、書き換え終了後前記フラッシュＲＯＭからの第２の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データを暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、終了通知信号を受けると保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュＲＯＭと；

前記暗号化した出力データを入力し、第１の回路データを前記フラッシュＲＯＭに出力し、この第１の回路データによりフラッシュＲＯＭのデータを書き換え、書き換え終了後前記フラッシュＲＯＭからの第２の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データの暗号を復号化した出力データを出力する可変処理回路と；

を有することを特徴とする請求項３、４又は５記載の暗号復号化装置。

【請求項７】　前記送信装置が、

前記入力データを入力し、回路データを生成出力する回路データ抽出部と；

前記入力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記入力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより暗号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって暗号化を行った出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化を行った出力データを入力し、回路データを生成出力する回路データ抽出部と；

前記出力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記暗号化を行った出力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより復号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって復号化を行った出力データを出力する可変処理回路と；

を有することを特徴とする請求項３、４又は５記載の暗号復号化装置。

【請求項８】　前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記入力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第１の回路データを生成出力するＦＰＧＡ回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記第１の回路データをもとに前記複数のＲＯＭから回路データを取り込み、暗号アルゴリズムを指定する第２の回路データを出力するセレクターと；

前記第２の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第２の回路データによって暗号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記暗号化した出力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第１の回路データを生成出力するＦＰＧＡ回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記第１の回路データをもとに前記複数のＲＯＭから回路データを取り込み、暗号アルゴリズムを指定する第２の回路データを出力するセレクターと；

前記第２の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第２の回路データによって復号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、復号化した出力データを出力する可変処理回路と；

を有することを特徴とする請求項３、４又は５記載の暗号復号化装置。

【請求項９】　前記複数のＲＯＭデータが、複数のハードウェア化されたデ

ータ回路からのデータであり、前記セレクターが出力する回路データを第１の回路データとして前記ＦＰＧＡ回路データ生成部に出力し、このＦＰＧＡ回路データ生成部が出力する第２の回路データを前記可変処理回路に出力することを特徴とする請求項８記載の暗号復号化装置。

【請求項１０】　前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクター制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記セレクター制御信号をもとに前記複数のＲＯＭを選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクターと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって暗号化を行い、暗号化した出力データを送出する可変処理回路と；

を有し、

前記受信装置は、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクター制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記セレクター制御信号をもとに前記複数のＲＯＭを選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクターと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの

送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって復号化を行い、復号化した出力データを送出する可変処理回路と；

を有することを特徴とする請求項３、４又は５記載の暗号復号化装置。

【請求項１１】　前記複数のＲＯＭデータが、複数のハードウェア化されたデータ回路部からのデータであり、前記ランダム発生器が、ある期間毎にセレクター制御信号を生成出力するタイマーであり、前記セレクターが出力する回路データを第１の回路データとして前記ＦＰＧＡ回路データ生成部に出力し、このＦＰＧＡ回路データ生成部が出力する第２の回路データを前記可変処理回路に出力することを特徴とする請求項８記載の暗号復号化装置。

【請求項１２】　前記可変処理回路が、フィールド・プログラマブル・ゲートアレイ（ＦＰＧＡ）であることを特徴とする請求項３、４、５、６、７、８又は１０記載の暗号復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号復号化装置に関し、特に暗号解読アルゴリズムを可変できる暗号復号化装置に関する。

【０００２】

【従来の技術】

最近は、携帯電話など無線を利用した通信技術が急速に発達しており、盗聴などによる通信データの漏洩防止が課題となっている。このため、通信データに暗号化処理を行い伝送することが一般に行われるが、暗号化復号化装置による暗号化復号化は、暗号鍵と通信データを決められたアルゴリズムの演算を繰り返すことで実行されるので、演算回数を増やすことで解読難易度が向上するが、新たに処理能力が問題となる。また、マルチメディア機器の急速な普及に伴い、通信データ量が急激に増加し処理能力問題に拍車をかけているため、ほとんどの暗号化

復号化装置では、演算をハードウェアで行うことにより対応しているのが現状である。このため、暗号鍵を変更する場合ハードウェアの変更が必要となる。

【０００３】

このような暗号化復号化技術の一例として、特開平５－１１０５５８号公報記載の「暗号処理装置」が知られている。

【０００４】

この公報では、データを暗号化し、この暗号化したデータを復号化する処理プログラムの一部又は全部をＥＥＰＲＯＭに格納し、暗号が解読された場合外部からの通信手段によりＥＥＰＲＯＭのプログラムを一部又は全部を書き換える技術が記載されている。

【０００５】

【発明が解決しようとする課題】

上述した従来の暗号復号化装置は、アルゴリズムの演算内容が漏洩または解読された場合に通信データは簡単に復号化されてしまうこと、常に同じアルゴリズムで演算を行っているために解読法が比較的短時間で見いだされるという欠点を有している。

【０００６】

また、暗号解読のアルゴリズムの変更は、ハードウェアの作り直しが必要であり早急な対応ができないこと、外部からの通信手段を用いてプログラムの書き換えを行うと暗号解読プログラムデータ漏洩の危険性があるという欠点を有している。

【０００７】

本発明の目的は、暗号化及び復号化の処理を全てハードウェアにより高速処理し、かつ暗号解読アルゴリズムのハードウェアの変更を可能とした暗号復号化装置を提供することにある。

【０００８】

【課題を解決するための手段】

本発明の暗号復号化装置は、データの暗号化と暗号化データの複合化を行う暗号復号化装置において、暗号化復号化する回路を可変可能な回路装置を用い、前

記可変可能な回路装置の回路データを秘密鍵として暗号化複合化を行うことを特徴としている。

【０００９】

前記可変可能な回路装置の回路データを複数個有し、暗号化複合化を行うための回路データ選択情報から、前記可変可能な回路装置の回路データを選択し供給することで異なるアルゴリズムの暗号化複合化を行うことを特徴としている。

【００１０】

入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきて前記暗号化データを入力し、暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は暗号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ＲＯＭ）とを有し、前記受信装置は復号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ＲＯＭ）とを有していることを特徴としている。

【００１１】

入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記書き換え情報の指示に従い前記複数のＲＯＭを選択し、選択したＲＯＭから暗号化する回路データを送出するセレクターと；

どのＲＯＭを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワー

ク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを、暗号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記書き換え情報の指示に従い前記複数のＲＯＭを選択し、選択したＲＯＭから復号化する回路データを送出するセレクターと；

どのＲＯＭを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記暗号化データを、復号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有することを特徴としている。

【００１２】

入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、解析データを出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成

を変更する第１の回路データを入力し、第２の回路データを生成出力するフィールド・プログラマブル・ゲートアレイ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ：以下ＦＰＧＡと記す）回路データ生成部と；

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号化する前記第１の回路データを前記ＦＰＧＡ回路データ生成部に出力するセレクターと；

前記ＦＰＧＡ回路データ生成部が出力する前記第２の回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワーク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、解析データを出力するデータ解析部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成を変更する第１の回路データを入力し、第２の回路データを生成出力するＦＰＧＡ回路データ生成部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号を復号化する前記第１の回路データを前記ＦＰＧＡ回路データ生成部に出力するセレクターと；

前記ＦＰＧＡ回路データ生成部が出力する前記第２の回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記

入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有することを特徴としている。

【００１３】

前記送信装置が、

前記入力データを入力保持し、終了通知信号を受けると保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュＲＯＭと；

前記入力データを入力し、第１の回路データを前記フラッシュＲＯＭに出力し、この第１の回路データによりフラッシュＲＯＭのデータを書き換え、書き換え終了後前記フラッシュＲＯＭからの第２の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データを暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、終了通知信号を受けると保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュＲＯＭと；

前記暗号化した出力データを入力し、第１の回路データを前記フラッシュＲＯＭに出力し、この第１の回路データによりフラッシュＲＯＭのデータを書き換え、書き換え終了後前記フラッシュＲＯＭからの第２の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データの暗号を復号化した出力データを出力する可変処理回路と；

を有することを特徴としている。

【００１４】

前記送信装置が、

前記入力データを入力し、回路データを生成出力する回路データ抽出部と；

前記入力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記入力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより暗号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって暗号化を行った出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化を行った出力データを入力し、回路データを生成出力する回路データ抽出部と；

前記出力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記暗号化を行った出力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより復号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって復号化を行った出力データを出力する可変処理回路と；

を有することを特徴としている。

【００１５】

前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記入力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第１の回路データを生成出力するＦＰＧＡ回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記第１の回路データをもとに前記複数のＲＯＭから回路データを取り込み、暗号アルゴリズムを指定する第２の回路データを出力するセレクターと；

前記第２の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第２の回路データによって暗号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記暗号化した出力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第１の回路データを生成出力するＦＰＧＡ回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記第１の回路データをもとに前記複数のＲＯＭから回路データを取り込み、暗号アルゴリズムを指定する第２の回路データを出力するセレクターと；

前記第２の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第２の回路データによって復号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、復号化した出力データを出力する可変処理回路と；

を有することを特徴としている。

【００１６】

前記複数のＲＯＭデータが、複数のハードウェア化されたデータ回路からのデータであり、前記セレクターが出力する回路データを第１の回路データとして前記ＦＰＧＡ回路データ生成部に出力し、このＦＰＧＡ回路データ生成部が出力する第２の回路データを前記可変処理回路に出力することを特徴としている。

【００１７】

前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクター制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記セレクター制御信号をもとに前記複数のＲＯＭを選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクターと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって暗号化を行い、暗号化した出力データを送出する可変処理回路と；

を有し、

前記受信装置は、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクター制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数のＲＯＭと；

前記セレクター制御信号をもとに前記複数のＲＯＭを選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクターと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって復号化を行い、復号化した出力データを送出する可変処理回路と；

を有することを特徴としている。

【００１８】

前記複数のＲＯＭデータが、複数のハードウェア化されたデータ回路部からのデータであり、前記ランダム発生器が、ある期間毎にセレクター制御信号を生成出力するタイマーであり、前記セレクターが出力する回路データを第１の回路データとして前記ＦＰＧＡ回路データ生成部に出力し、このＦＰＧＡ回路データ生成部が出力する第２の回路データを前記可変処理回路に出力することを特徴としている。

【００１９】

また、前記可変処理回路が、フィールド・プログラマブル・ゲートアレイ（ＦＰＧＡ）であることを特徴としている。

【００２０】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。

【００２１】

図１は本発明の暗号復号化装置の一つの実施の形態を示すブロック図である。

【００２２】

図１に示す本実施の形態は、入力データ１０１を暗号化し暗号化データ１１０を出力する送信装置１０２と、暗号化データ１１０を伝送するネットワーク網１１１と、このネットワーク網１１１を介して伝送されてきて暗号化データ１１３を入力し、暗号解読を行い復号化した出力データ１１２を出力する受信装置１０６とから構成されている。

【００２３】

なお、送信装置１０２は暗号化する可変処理回路１０３と、この可変処理回路１０３に秘密鍵の回路データ１０５を出力するリード・オンリー・メモリであるＲＯＭ１０４とを有し、受信装置１０６は復号化する可変処理回路１０７と、この可変処理回路１０７に秘密鍵の回路データ１０９を出力するリード・オンリー・メモリであるＲＯＭ１０８とを有している。

【００２４】

なお、上述の可変処理回路１０３，１０７は具体的な回路素子としてＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）が使用され、任意の回路構成がプログラムデータの変更により容易に実現できる。

【００２５】

次に動作を説明する。

【００２６】

入力データ１０１は可変処理回路１０３により暗号化され、この暗号化された暗号化データ１１０は一般的なネットワーク網１１１に供給される。受信装置１０６はネットワーク網１１１から暗号化データ１１３を入力する。暗号化データ１１３は、復号化のため可変処理回路１０７で復号化処理がなされ、出力データ１１２として出力される。

【００２７】

なお、ＲＯＭ１０４は秘密鍵を変更する場合に取り替えて、可変処理回路１０３の書き換えを行う。取り替えられたＲＯＭ１０４から新しい暗号化アルゴリズムを生成する回路データ１０５が可変処理回路１０３に出力され、可変処理回路１０３の回路構成を変更することにより、入力データ１０１は新しい形式の暗号化データ１１０が出力される。新しい形式の暗号化データ１１０に対し、受信装置１０６の可変処理回路１０７も新しいＲＯＭ１０８を用いて回路構成を変更し、新しい形式の暗号化データ１１３の復号化を行う。

【００２８】

つまり、可変処理回路１０３，１０７の回路変更は取り替え可能なＲＯＭ１０４，１０８が出力する回路データ１０５，１０９により行われる。

【００２９】

上述の通り、送信装置１０２には、暗号化する可変処理回路１０３と回路データ１０５が記憶されているＲＯＭ１０４とを有しており、送信装置１０２を起動させたとき、ＲＯＭ１０４から回路データ１０５が暗号化する可変処理回路１０３へ送出される。回路データ１０５によって暗号化する可変処理回路１０３の回路構成が新しく形成され、入力データ１０１を順次暗号化する可変処理回路１０３となる。この暗号化する可変処理回路１０３によって暗号化された暗号化データ１１０は、ネットワーク網１１１に送出される。

【００３０】

受信装置１０６も同様に復号化する可変処理回路１０７と回路データ１０９が記憶されているＲＯＭ１０８とを有しており、受信装置１０６を起動させたとき、ＲＯＭ１０８から回路データ１０９が復号化する可変処理回路１０７へ送出される。回路データ１０９によって復号化する可変処理回路１０７の回路構成が新しく形成され、暗号化データ１１３を順次復号化する可変処理回路１０７となる。この可変処理回路１０７により、ネットワーク網１１１から受信した暗号化データ１１３を復号化し、出力データ１１２を生成出力する。

【００３１】

ＲＯＭ１０４，ＲＯＭ１０８は、秘密鍵を変更する場合に取り替えて、暗号化する可変処理回路１０３、復号化する可変処理回路１０７の書き換えデータを各々生成する。こうして生成された回路データ１０５，１０９は暗号化する可変処理回路１０３、復号化する可変処理回路１０７に出力され、回路構成を変更することにより新しい形式の暗号化および復号化に対応することになる。

【００３２】

図２は本発明の暗号復号化装置の一例を示す詳細ブロック図である。

【００３３】

なお、図２において図１に示す構成要素に対応するものは同一の参照数字または符号を付し、その説明を省略する。

【００３４】

図２を参照すると、入力データ２０２を暗号化し暗号化データ２１１を出力する送信装置２０１と、暗号化データ２１１を伝送するネットワーク網１１１と、

このネットワーク網１１１を介して伝送されてきて暗号化データ２１３を入力し、暗号解読を行い復号化した出力データ２１４を出力する受信装置２０１ａとから構成されている。

【００３５】

なお、送信装置２０１に入力する入力データ２０２は、決められた指定に従い書き換え情報が付随した信号である。

【００３６】

入力データ２０２は、データ解析部２０３と暗号／復号化データ保持部２０４に出力される。データ解析部２０３では、決められた指定通りに情報を解析し、デコードして書き換え情報２１６をセレクター２０５に出力する。セレクター２０５は、書き換え情報２１６の指示に従いＲＯＭ２０６，２０６ａ，２０６ｂ，２０６ｎを選択し、暗号化する可変処理回路２０７に回路データ２０８を送出する。暗号化する可変処理回路２０７では、回路データ２０８をもとにして、暗号化する可変処理回路２０７の内部回路を書き換え、どのＲＯＭを選択するかにより暗号アルゴリズムを選択することができる。暗号化する可変処理回路２０７で回路変更が完了すると、可変処理回路２０７は終了通知信号２０９を暗号／復号化データ保持部２０４に出力する。終了通知信号２０９を受けた暗号／復号化データ保持部２０４は、それまで保持していた入力データ２０２を暗号化する可変処理回路２０７に入力保持データ２１０として出力する。こうして、可変処理回路２０７は入力データ２０２の暗号化を行い、暗号化データ２１１をネットワーク網１１１に送出する。

【００３７】

ネットワーク網１１１から入力された暗号化データ２１３は、データ解析部２０３ａと暗号／復号化データ保持部２０４ａに送出される。データ解析部２０３ａでは、決められた指定通りに情報を解析し、デコードして書き換え情報２１６ａをセレクター２０５ａに出力する。セレクター２０５ａは、書き換え情報２１６ａの指示に従いＲＯＭ２１５，２１５ａ，２１５ｂ，２１５ｎを選択し、復号化する可変処理回路２０７ａに回路データ２０８ａを出力する。復号化する可変処理回路２０７ａでは、回路データ２０８ａをもとに暗号を復号化する可変処理

回路２０７ａの内部回路を書き換える。復号化する可変処理回路２０７ａで回路変更が完了すると、終了通知信号２０９ａを暗号／復号化データ保持部２０４ａに出力する。終了通知信号２０９ａを受けた暗号／復号化データ保持部２０４ａは、それまで保持していた暗号化データ２１３を復号化する可変処理回路２０７ａに入力保持データ２１０ａとして出力する。かくして、可変処理回路２０７ａは暗号化データ２１３の復号化を行い出力データ２１４を出力する。

【００３８】

図３は図２の動作を示すタイムチャートである。

【００３９】

次に、図２および図３を参照して本実施の形態の動作をより詳細に説明する。

【００４０】

入力データ２０２はヘッダ情報と暗号化するデータ信号とからなり、データ解析部２０３は入力データ２０２から書き換え情報２１６を抽出すると、書き換え情報２１６のデータをデコードしてセレクター２０５を制御する。

【００４１】

これによって、ＲＯＭ２０６，２０６ａ，２０６ｂ，２０６ｎのデータを切り替え、回路データ２０８を生成する。ＲＯＭのデータを切り換えると同時に可変処理回路２０７に書き換え信号を生成し、暗号化する可変処理回路２０７は可変処理回路２０７の書き換え信号の立ち上がりで初期化する。暗号化する可変処理回路２０７は回路データ２０８をもとに回路を変更し、変更が終わると終了通知信号２０９を出力する。終了通知信号２０９を受けるまで暗号／復号化データ保持部２０４では入力データ２０２を保持し、この保持していた保持データ２１０を入力された順に暗号化する可変処理回路２０７に送出する。暗号化する可変処理回路２０７により保持データ２１０の暗号化の処理を行い暗号化データ２１１を生成出力する。

【００４２】

図４は図２の全体動作を示すフローチャートである。

【００４３】

入力データ２０２を受けると暗号／復号化動作を行う（ステップ１：Ｓ１）。

【００４４】

ステップ２（Ｓ２）で書き換え情報２１６，２１６ａ受信の判定を行い、書き換え情報２１６，２１６ａを受信するまではステップ１に戻り、暗号／復号化動作を繰り返す。ステップ２で書き換え情報を受信すると、受信した書き換え情報２１６，２１６ａに対してデコードする（ステップ３：Ｓ３）。

【００４５】

次にセレクター２０５，２０５ａの制御を行い、暗号／復号化する可変処理回路２０７，２０７ａに書き換え信号を送出し、また暗号／復号化データ保持部２０４，２０４ａにデータの保持を開始させる（ステップ４：Ｓ４）。その後、セレクター２０５，２０５ａによって選択された回路データを暗号／復号化する可変処理回路２０７，２０７ａに送出する（ステップ５：Ｓ５）。次のステップ６（Ｓ６）で暗号／復号化する可変処理回路２０７，２０７ａの書き換えが完了したかの判断を行い、完了していない場合ステップ１（Ｓ１）に戻り、完了している場合ステップ７（Ｓ７）に進み終了通知信号２０９，２０９ａを生成し、暗号／復号化する可変処理回路２０７，２０７ａの書き換え信号をリセットする。また、暗号／復号化データ保持部２０４，２０４ａで保持していた信号を暗号／復号化する可変処理回路２０７，２０７ａにデータを送出開始する（ステップ８：Ｓ８）。

【００４６】

上述の通り、回路データ２０８，２０８ａを秘密鍵としているので、回路データをもった送受信機のみ解読可能な暗号通信が可能となる。従ってセキュリティの向上を図ることができる。さらに、複数のＲＯＭデータが設けられているので、通信毎に暗号鍵を変更できることになる。この結果、一つのデータを複数の回路構成によって暗号化することができる。秘密鍵が回路データとなっているので、万一秘密鍵が漏れても同様の回路構成を作る事が困難であるため、より高度な暗号回路が構成できることになる。

【００４７】

図５は本発明の暗号復号化装置の第２の実施の形態を示す詳細ブロック図である。

【００４８】

なお、図５において図２に示す構成要素に対応するものは同一の参照数字または符号を付し、その説明を省略する。

【００４９】

図５を参照すると、入力データ３０３を暗号化し暗号化データ３１４を出力する送信装置３０２と、暗号化データ３１４を伝送するネットワーク網１１１と、このネットワーク網１１１を介して伝送されてきて暗号化データ３１５を入力し、暗号解読を行い復号化した出力データ３１６を出力する受信装置３０２ａとから構成されている。

【００５０】

送信装置３０２に入力する入力データ３０３は、決められた指定に従い書き換え情報が付随した送受信信号である。入力データ３０３は、データ解析部３０４と暗号／復号化データ保持部３０５に送出される。データ解析部３０４では、決められた指定通りに情報を解析し、解析データ３１７をＦＰＧＡ回路データ生成部３０６に送出する。ＦＰＧＡは既述の通り、Ｆｉｅｌｄ　Ｐｒｏｇｒａｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙの素子で、ＦＰＧＡ回路データ生成部３０６は可変処理回路３０１の回路構成を変更する回路データを生成する。

【００５１】

ＦＰＧＡ回路データ生成部３０６では、データ解析部３０４からの解析データ３１７をもとに選択信号３０８をセレクター３０９に出力し、データ回路部３０７，３０７ａ，３０７ｂ，３０７ｎを選択する。選択信号３０８により、書き換え情報の要求通りに組み合わせた回路データ３１０をＦＰＧＡ回路データ生成部３０６に出力する。

【００５２】

暗号化する可変処理回路３０１では、ＦＰＧＡ回路データ生成部３０６が出力する回路データ３１１をもとに回路を変更する。可変処理回路３０１で回路変更が終了すると、終了通知信号３１２を暗号／復号化データ保持部３０５に出力する。終了通知信号３１２を受けた暗号／復号化データ保持部３０５は、入力データ３０３を新たに入力保持データ３１３として頭から可変処理回路３０１に送出

する。入力保持データ３１３を受信した可変処理回路３０１は、書き換えた回路によって暗号化を行う。こうして、可変処理回路３０１は暗号化を行い暗号化データ３１４をネットワーク網１１１に送出する。

【００５３】

ネットワーク網１１１から入力された暗号化データ３１５は、データ解析部３０４ａと暗号／復号化データ保持部３０５ａに送出される。データ解析部３０４ａでは、決められた指定通りに情報を解析し、解析データ３１７ａをＦＰＧＡ回路データ生成部３０６ａに送出する。ＦＰＧＡ回路データ生成部３０６ａでは、データ解析部３０４ａからの解析データ３１７ａをもとに選択信号３０８ａをセレクター３０９ａに送り、データ回路部３１６，３１６ａ，３１６ｂ，３１６ｎを選択する。選択信号３０８ａにより、書き換え情報の要求通りに組み合わせた回路データ３１０ａをＦＰＧＡ回路データ生成部３０６ａに出力する。復号化する可変処理回路３０１ａでは、ＦＰＧＡ回路データ生成部３０６ａが出力する回路データ３１１ａをもとに回路を変更する。可変処理回路３０１ａで回路変更が終了すると、終了通知信号３１２ａを暗号／復号化データ保持部３０５ａに出力する。終了通知信号３１２ａを受けた暗号／復号化データ保持部３０５ａは、入力データ３０３ａを新たに入力保持データ３１３ａとして頭から可変処理回路３０１ａに送出する。入力保持データ３１３ａを受信した可変処理回路３０１ａは、書き換えた回路によって復号化を行う。かくして、可変処理回路３０１ａは復号化を行い出力データ３１６を出力する。

【００５４】

上述の通り本第２の実施の形態はＲＯＭ回路からのＲＯＭデータとは異なり、複数個用意されたデータ回路部３０７，３０７ａ，３０７ｂ，３０７ｎを書き換え情報に従って組み合わせ、一つの回路構成を形成するようにしたものである。

【００５５】

送信装置３０２に入力する入力データ３０３は、決められた指定に従い書き換え情報を付随した信号であり、入力データ３０３は、データ解析部３０４と暗号／復号化データ保持部３０５に送出される。データ解析部３０４では、決められた指定通りに情報を解析し、解析データ３１７をＦＰＧＡ回路データ生成部３０

６に送出する。ＦＰＧＡ回路データ生成部３０６では、データ解析部３０４からの解析データ３１７をもとにデータ回路部３０７，３０７ａ，３０７ｂ，３０７ｎを任意に選択する。選択信号３０８をセレクター３０９に送り、回路データ３１０を書き換え情報の要求通りに組み合わせて、可変処理回路３０１のデータの生成を行う。暗号化する可変処理回路３０１では、その組み合わせて作り出された回路データ３１１をもとに回路を変更する。暗号化する可変処理回路３０１で回路変更が終了すると、終了通知信号３１２を暗号／復号化データ保持部３０５に出力する。終了通知信号３１２を受けた暗号／復号化データ保持部３０５は、入力データ３０３を暗号化する可変処理回路３０１に頭から送出する。入力保持データ３１３を受信した暗号化する可変処理回路３０１は、書き換えた回路によって暗号復号化を行う。これにより、データの数の組み合わせ分だけの暗号復号化の回路構成を生成できる。

【００５６】

図６は本発明の暗号復号化装置の第３の実施の形態を示すブロック図である。

【００５７】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網１１１を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一活表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【００５８】

図６を参照すると、暗号復号化装置４０１に入力する入力データ４０２を暗号／復号化する可変処理回路４０３に入力し、同時に暗号／復号化データ保持部４０４に保持しておく。暗号／復号化する可変処理回路４０３によって、回路データ４０５を抽出し、ＦＬＡＳＨ　ＲＯＭ４０６を書き換える。ＦＬＡＳＨ　ＲＯＭ４０６の書き換えが終了したら、暗号／復号化する可変処理回路４０３をリセットしＦＬＡＳＨ　ＲＯＭ４０６に書き込まれた回路データ４０７を読み出し可変処理回路４０３の内部回路を変更する。暗号／復号化する可変処理回路４０３の内部回路が生成完了したら、暗号／復号化データ保持部４０４に終了通知信号４０８を送出する。暗号／復号化データ保持回路４０４で保持しておいた保持デ

ータ４０９を暗号／復号化する可変処理回路４０３を通して、暗号復号化を行った出力データ４１０を送出する。

【００５９】

このように、本形態では多数の暗号アルゴリズムを決定する回路データにより変更できることになる。

【００６０】

図７は本発明の暗号復号化装置の第４の実施の形態を示すブロック図である。

【００６１】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網１１１を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一活表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【００６２】

図７を参照すると、暗号復号化装置５０１に入力する入力データ５０２を、回路データ抽出部５０３で予め定めておいたフォーマットに従って抽出し、回路データ５０４を生成する。この回路データ５０４により、暗号／復号化する可変処理回路５０５の回路変更を行う。入力データ５０２は、暗号／復号化データ保持部５０６に回路変更終了まで保持しておき、暗号／復号化データ保持部５０６が終了通知信号５０７を受けると、暗号／復号化する可変処理回路５０５へ保持していた保持データ５０９を送出し、暗号／復号化する可変処理回路５０５の新しい回路構成によって暗号復号化を行い出力データ５０８を出力する。

【００６３】

図８は本発明の暗号復号化装置の第５の実施の形態を示すブロック図である。

【００６４】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網１１１を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一活表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【００６５】

図８を参照すると、暗号復号化装置６０１に入力する入力データ６０２は、暗号／復号化データ保持部６０３に一度保持される。データ解析部６０４では、入力された入力データ６０２が暗号化したいデータであるか復号化したいデータであるかを判定する。データ解析部６０４は暗号化したいデータである場合は、ランダム発生器６０６からのデータを有効にするようにＦＰＧＡ回路データ生成部６０５に通知し、復号化したいデータである場合は、データ解析部６０４で抽出した暗号鍵を有効にするようにＦＰＧＡ回路データ生成部６０５に通知すると共に抽出した暗号鍵を送出する。ＦＰＧＡ回路データ生成部６０５では、データ解析部６０４からの解析データ６１４の通知に従い可変処理回路６１０のための回路データ６１５を生成する。ランダム発生器６０６からの信号を有効にして可変処理回路６１０の回路データ６０９を生成する場合は、ランダム発生器６０６からの信号を取り込み、そのデータをもとにセレクター６０７を制御し、ＲＯＭ６０８，６０８ａ，６０８ｂ，６０８ｎから回路データを取り込み、回路データを組み合わせて回路データ６０９を生成する。回路データ６０９を受信した可変処理回路６１０は、暗号／復号化データ保持部６０３からの保持データ６１１の送出を止めるように回路変更通知信号６１２を出力し、回路データ６０９によって暗号／復号化する可変処理回路６１０の内部の構成を変更する。変更が終了すると回路変更通知信号６１２を停止し、再び暗号／復号化データ保持部６０３からの保持データ６１１を送出してもらう。新しい回路構成となった暗号／復号化する可変処理回路６１０は暗号復号化を行い、出力データ６１３を送出する。

【００６６】

上述の通り、書き換え情報の生成をランダム発生器６０６に任せることでシステムへの負荷の軽減を図ったものである。

【００６７】

図９は本発明の暗号復号化装置の第６の実施の形態を示すブロック図である。

【００６８】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網１１１を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一活表示にして説明の簡略化を図る。送信装置は暗号化、受信装

置は復号化として暗号／復号化を読み替えるものとする。

【００６９】

図９を参照すると、暗号復号化装置７０１に入力する入力データ７０２は、暗号／復号化データ保持部７０３に一旦収納される。データ解析部７０４では、入力された入力データ７０２が暗号化したいデータであるか復号化したいデータであるかを判定する。暗号化したいデータである場合は、ランダム発生器７０６からのデータを有効にするようにＦＰＧＡ回路データ生成部７０５に通知し、復号化したいデータである場合は、データ解析部７０４で抽出した暗号鍵を有効にするようにＦＰＧＡ回路データ生成部７０５に通知すると共に抽出した暗号鍵を送出する。ＦＰＧＡ回路データ生成部７０５では、データ解析部７０４からの解析データ７１４の通知に従いＦＰＧＡの回路データを生成する。ランダム発生器７０６からの信号を有効にしてＦＰＧＡの回路データを生成する場合は、ランダム発生器７０６からの信号を取り込み、そのデータをもとにセレクター７０７を制御し、データ回路部７０８，７０８ａ，７０８ｂ，７０８ｎから回路データ７１５を取り込み、回路データ７１５を組み合わせて回路データ７０９を生成する。回路データ７０９を受信した可変処理回路７１０は、暗号／復号化データ保持部７０３からの保持データ７１１の送出を止めるように回路変更通知信号７１２によって連絡し、ＦＰＧＡ用回路データ７０９によって暗号／復号化する可変処理回路７１０の内部の構成を変更する。変更が終了すると回路変更通知信号７１２を停止し、再び暗号／復号化データ保持部７０３からの保持データ７１１を送出してもらい、新しい回路構成となった暗号／復号化する可変処理回路７１０は暗号復号化を行い、出力データ７１３を送出する。これにより、よりハードウェア化されるため、システムでの負荷を最小限に抑えられると同時により多くの暗号鍵を備えることになる。

【００７０】

図１０は本発明の暗号復号化装置の第７の実施の形態を示すブロック図である。

【００７１】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネ

ットワーク網１１１を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一活表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【００７２】

図１０を参照すると、暗号復号化装置８０１に入力する入力データ８０２は、暗号／復号化データ保持部８０３に一度保持される。暗号／復号化データ保持部８０３では、暗号／復号化する可変処理回路８０４からの回路変更通知信号８０５によって出力を停止されている場合を除いて、常に暗号／復号化する可変処理回路８０４へ保持データ８０６を送出する。暗号／復号化する可変処理回路８０４では、暗号／復号化データ保持部８０３からの保持データ８０６を内部の回路構成によって暗号復号化を行い出力データ８０７を送出する。タイマー８０８は、ある期間毎にセレクター８０９を制御するセレクター制御信号８１２を生成する。セレクター８０９では、タイマー８０８からのセレクター制御信号８１２をもとにＲＯＭ８１０，８１０ａ，８１０ｂ，８１０ｎを選択し、暗号／復号化する可変処理回路８０４に回路データ８１１を送出する。回路データ８１１を受けた暗号／復号化する可変処理回路８０４は、一旦出力データ８０７の生成を止め、回路変更通知信号８０５を暗号／復号化データ保持部８０３に送り、保持データ８０６の送出を停止させる。暗号／復号化する可変処理回路８０４は、回路データ８１１をもとに内部の回路構成を変更し、変更が終了すると暗号／復号化データ保持部８０３に保持データ８０６の送出を再開させるべく、回路変更通知信号８０５を止めて保持データ８０６を入力する。暗号／復号化する可変処理回路８０４は、変更した内部の回路構成によって暗号復号化を行い、出力データ８０７を送出する。これにより、暗号解読のキーワードを全く送出しなくなるため、第三者による暗号解読がより困難になる。

【００７３】

送受信側に同期を取ったタイマーを備えることでより機密性の高いを構成としている。

【００７４】

図１１は本発明の暗号復号化装置の第８の実施の形態を示すブロック図である

【００７５】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網１１１を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一活表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【００７６】

図１１を参照すると、暗号復号化装置９０１に入力する入力データ９０２は、暗号／復号化データ保持部９０３に一度保持される。暗号／復号化データ保持部９０３では、暗号／復号化する可変処理回路９０４からの回路変更通知信号９０５によって出力を停止されている場合を除いて、常に暗号／復号化する可変処理回路９０４へ保持データ９０６を送出する。暗号／復号化する可変処理回路９０４では、暗号／復号化データ保持部９０３からの保持データ９０６を内部の回路構成によって暗号復号化を行い出力データ９０７を送出する。

【００７７】

タイマー９０８は、ある期間毎にＦＰＧＡ回路データ生成部９０９に信号を送出する。ＦＰＧＡ回路データ生成部９０９では、タイマー９０８から受けた信号情報をもとに、セレクター９１０を制御し、選択されたデータ回路部９１１，９１１ａ，９１１ｂ，９１１ｎを取り込み、取り込んだ回路データ９１２を組み合わせ可変処理回路９０４の回路データ９１３を生成し、生成した回路データ９１３を暗号／復号化する可変処理回路９０４に送出する。回路データ９１３を入力した暗号／復号化する可変処理回路９０４は、一度出力データ９０７の生成を止め、回路変更通知信号９０５を暗号／復号化データ保持部９０３に送り、出力データ９０７の送出を停止させ、暗号／復号化する可変処理回路９０４は、回路データ９１３をもとに内部の回路構成を変更し、変更が終了すると暗号／復号化データ保持部９０３に保持データ９０６の送出を再開させる。回路変更通知信号９０５を止めて、保持データ９０６を入力する。暗号／復号化する可変処理回路９０４は、変更した内部の回路構成によって暗号復号化を行い、出力データ９０７を送出する。これにより、より機密性の高く、より柔軟性のある回路構成となる

ため、第三者による暗号解読は困難になる。

【００７８】

図１２は本発明の暗号復号化装置を利用したシステムブロック図である。

【００７９】

図１２を参照すると、親局１の秘密鍵管理部２から、定期的に暗号／復号化するＦＰＧＡ変更用のデータを子局３，４へ送出する。子局３，４側では、前回までの回路データを元にした可変処理回路５，６によって、回路データ７，８を認識し、ＦＬＡＳＨ　ＲＯＭ９，１０に書き込む。親局１側で更新通知を子局３，４全てに送出し、その通知が来るとＦＬＡＳＨ　ＲＯＭ９，１０に蓄えてあった回路データ７，８をもとに、子局３，４が一斉に暗号／復号化する可変処理回路５，６の回路構成を変更する。暗号／復号化する可変処理回路５，６は新しい秘密鍵によって通信の運用を行えるようになる。回路データ７，８は、通常の通信中に少しずつ送出しておくとともに、通常はダミービット扱いの信号としてＦＬＡＳＨ　ＲＯＭ９，１０内部を徐々に変更しておく。

【００８０】

図１３は可変処理回路による暗号復号化装置の一例を示すブロック図である。

【００８１】

図１３を参照にすると、暗号復号化装置１１は、入力データ１２を回路データ抽出部１３、回路データ保持部１４、暗号／復号化部１５の全てに入力されている。回路データ抽出部１３では、入力データ１２を保持し、内部情報を解析し回路データ１７を抽出する。抽出した回路データ１７を、回路データ保持部１４が保持しておき、回路データ１８として暗号／復号化部１５に送出する。暗号／復号化部１５では、回路データ保持部１４からの回路データ１８をもとに内部回路構成を変更する。変更が終了すると、回路データ抽出部１３で蓄えていた入力データ１２の暗号復号化の処理を行い、出力データ１６を生成出力する。

【００８２】

なお、ＦＬＡＳＨ　ＲＯＭを用いているが、この部分に可変処理回路を並べるという技術思想を用いても得られる。

【００８３】

つまり本装置のＦＬＡＳＨ　ＲＯＭ部にＦＰＧＡとしての可変処理回路を用い、また回路構成抽出部自身にもＦＰＧＡを使用している。従って、各ＦＰＧＡの回路構成を全て解読できなければ第三者が解読できないという作用が得られる。図１３において、暗号復号化装置１１は、３つのＦＰＧＡとして回路データ抽出部１３、回路データ保持部１４、暗号／復号化部１５を持つ。入力される入力データ１２は、回路データ抽出部１３、回路データ保持部１４、暗号／復号化部１５の全てのＦＰＧＡに入力される。回路データ抽出部１３では、回路情報の抽出を行う。回路データ保持部１４では、抽出した回路データ１７を保持しておく。暗号／復号化部１５では、回路データ保持部１４からの回路データ１８によって回路構成を変更する。

【００８４】

変更が完了すると、回路データ抽出部１３へ終了通知信号１９を出力する。終了通知信号１９を受信した回路データ抽出部１３は、保持していた保持データ２０を暗号／復号化部１５に送出する。暗号／復号化部１５では、新しい回路構成で暗号復号化し、データを送出する。これにより、暗号解読のためには、様々な要素を持つことになる。

【００８５】

本形態では、相互に回路データ抽出部を備えているので、一つのＦＰＧＡの回路変更がうまくいかなかった、あるいは、故障してしまっても他のＦＰＧＡで書き換えを可能にするという相乗的な効果を奏する。

【００８６】

本実施例のＦＰＧＡはＦＰＧＡ搭載の特定用途向け集積回路であるＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）に変更してもよい。さらに、複雑な回路構成をＡＳＩＣで実現できれば、より気密性の高いデータ転送に有効である。

【００８７】

【発明の効果】

以上説明したように、本発明の暗号復号化装置は、可変処理回路の回路データが可変できるので、処理能力を落とすことなく暗号アルゴリズムの演算を変更す

ることができるという効果を有している。

【００８８】

また、可変処理回路の回路データの変換アルゴリズムを非公開とすることでより難解な解読度が実現可能となり、暗号解読プログラムデータの漏洩を防ぐことができるという効果を有している。

【図面の簡単な説明】

【図１】

本発明の暗号復号化装置の一つの実施の形態を示すブロック図である。

【図２】

本発明の暗号復号化装置の一例を示す詳細ブロック図である。

【図３】

図２の動作を示すタイムチャートである。

【図４】

図２の全体動作を示すフローチャートである。

【図５】

本発明の暗号復号化装置の第２の実施の形態を示す詳細ブロック図である。

【図６】

本発明の暗号復号化装置の第３の実施の形態を示すブロック図である。

【図７】

本発明の暗号復号化装置の第４の実施の形態を示すブロック図である。

【図８】

本発明の暗号復号化装置の第５の実施の形態を示すブロック図である。

【図９】

本発明の暗号復号化装置の第６の実施の形態を示すブロック図である。

【図１０】

本発明の暗号復号化装置の第７の実施の形態を示すブロック図である。

【図１１】

本発明の暗号復号化装置の第８の実施の形態を示すブロック図である。

【図１２】

本発明の暗号復号化装置を利用したシステムブロック図である。

【図１３】

可変処理回路による暗号復号化装置の一例を示すブロック図である。

【符号の説明】

１　親局

２　秘密鍵管理部

３，４　子局

５，６　可変処理回路

７，８　回路データ

９，１０　ＦＬＡＳＨ　ＲＯＭ

１１　暗号復号化装置

１２　入力データ

１３　回路データ抽出部

１４　回路データ保持部

１５　暗号／復号化部

１６　出力データ

１７，１８　回路データ

１９　終了通知信号

２０　保持データ

１０１　入力データ

１０２　送信装置

１０３，１０７　可変処理回路

１０４，１０８　ＲＯＭ

１０５，１０９　回路データ

１０６　受信装置

１１０　暗号化データ

１１１　ネットワーク網

１１２　出力データ

１１３　暗号化データ

２０１　送信装置

２０１ａ　受信装置

２０２　入力データ

２０３，２０３ａ　データ解析部

２０４，２０４ａ　暗号／復号化データ保持部

２０５，２０５ａ　セレクター

２０６，２０６ａ，２０６ｂ，２０６ｎ　ＲＯＭ

２０７，２０７ａ　可変処理回路

２０８，２０８ａ　回路データ

２０９，２０９ａ　終了通知信号

２１０，２１０ａ　入力保持データ

２１１　暗号化データ

２１３　暗号化データ

２１４　出力データ

２１５，２１５ａ，２１５ｂ，２１５ｎ　ＲＯＭ

２１６，２１６ａ　書き換え情報

３０１，３０１ａ　可変処理回路

３０２　送信装置

３０２ａ　受信装置

３０３　入力データ

３０４，３０４ａ　データ解析部

３０５，３０５ａ　暗号／復号化データ保持部

３０６，３０６ａ　ＦＰＧＡ回路データ生成部

３０７，３０７ａ，３０７ｂ，３０７ｎ　データ回路部

３０８，３０８ａ　選択信号

３０９，３０９ａ　セレクター

３１０，３１０ａ　回路データ

３１１，３１１ａ　回路データ

３１２，３１２ａ　終了通知信号

３１３，３１３ａ　入力保持データ

３１４，３１５　暗号化データ

３１６，３１６ａ，３１６ｂ，３１６ｎ　データ回路部

３１７，３１７ａ　解析データ

４０１　暗号復号化装置

４０２　入力データ

４０３　可変処理回路

４０４　暗号／復号化データ保持部

４０５　回路データ

４０６　ＦＬＡＳＨ　ＲＯＭ

４０７　回路データ

４０８　終了通知信号

４０９　保持データ

４１０　出力データ

５０１　暗号復号化装置

５０２　入力データ

５０３　回路データ抽出部

５０４　回路データ

５０５　可変処理回路

５０６　暗号／復号化データ保持部

５０７　終了通知信号

５０８　出力データ

５０９　保持データ

６０１　暗号復号化装置

６０２　入力データ

６０３　暗号／復号化データ保持部

６０４　データ解析部

６０５　ＦＰＧＡ回路データ生成部

６０６　ランダム発生器

６０７　セレクター

６０８，６０８ａ，６０８ｂ，６０８ｎ　ＲＯＭ

６０９　回路データ

６１０　可変処理回路

６１１　保持データ

６１２　回路変更通知信号

６１３　出力データ

６１４　解析データ

６１５　回路データ

７０１　暗号復号化装置

７０２　入力データ

７０３　暗号／復号化データ保持部

７０４　データ解析部

７０５　ＦＰＧＡ回路データ生成部

７０６　ランダム発生器

７０７　セレクター

７０８，７０８ａ，７０８ｂ，７０８ｎ　データ回路部

７０９　回路データ

７１０　可変処理回路

７１１　保持データ

７１２　回路変更通知信号

７１３　出力データ

７１４　解析データ

７１５　回路データ

８０１　暗号復号化装置

８０２　入力データ

８０３　暗号／復号化データ保持部

８０４　可変処理回路

８０５　回路変更通知信号

８０６　保持データ

８０７　出力データ

８０８　タイマー

８０９　セレクター

８１０，８１０ａ，８１０ｂ，８１０ｎ　ＲＯＭ

８１１　回路データ

８１２　セレクター制御信号

９０１　暗号復号化装置

９０２　入力データ

９０３　暗号／復号化データ保持部

９０４　可変処理回路

９０５　回路変更通知信号

９０６　保持データ

９０７　出力データ

９０８　タイマー

９０９　ＦＰＧＡ回路データ生成部

９１０　セレクター

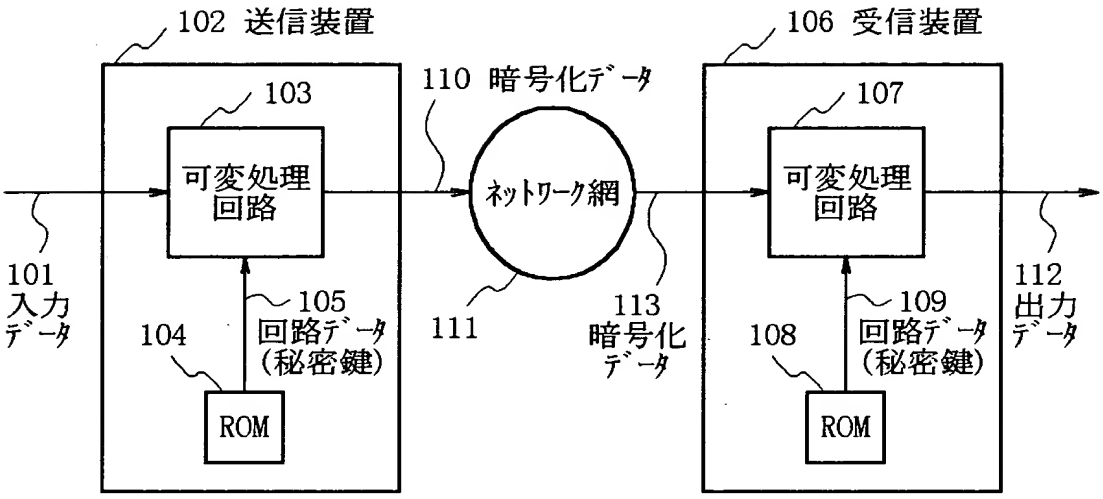
９１１，９１１ａ，９１１ｂ，９１１ｎ　データ回路部

９１２　回路データ

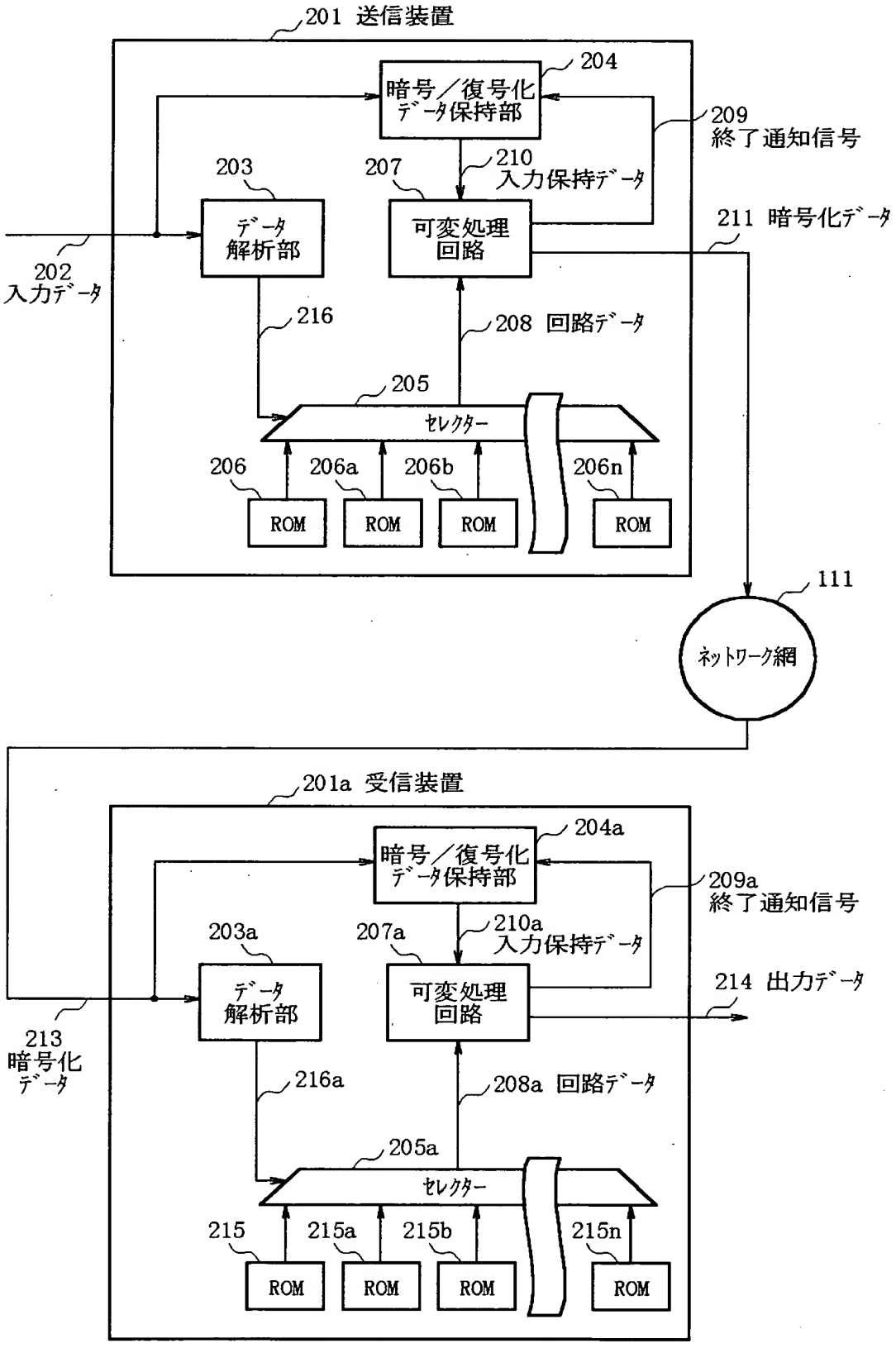
９１３　回路データ

【書類名】　　図面

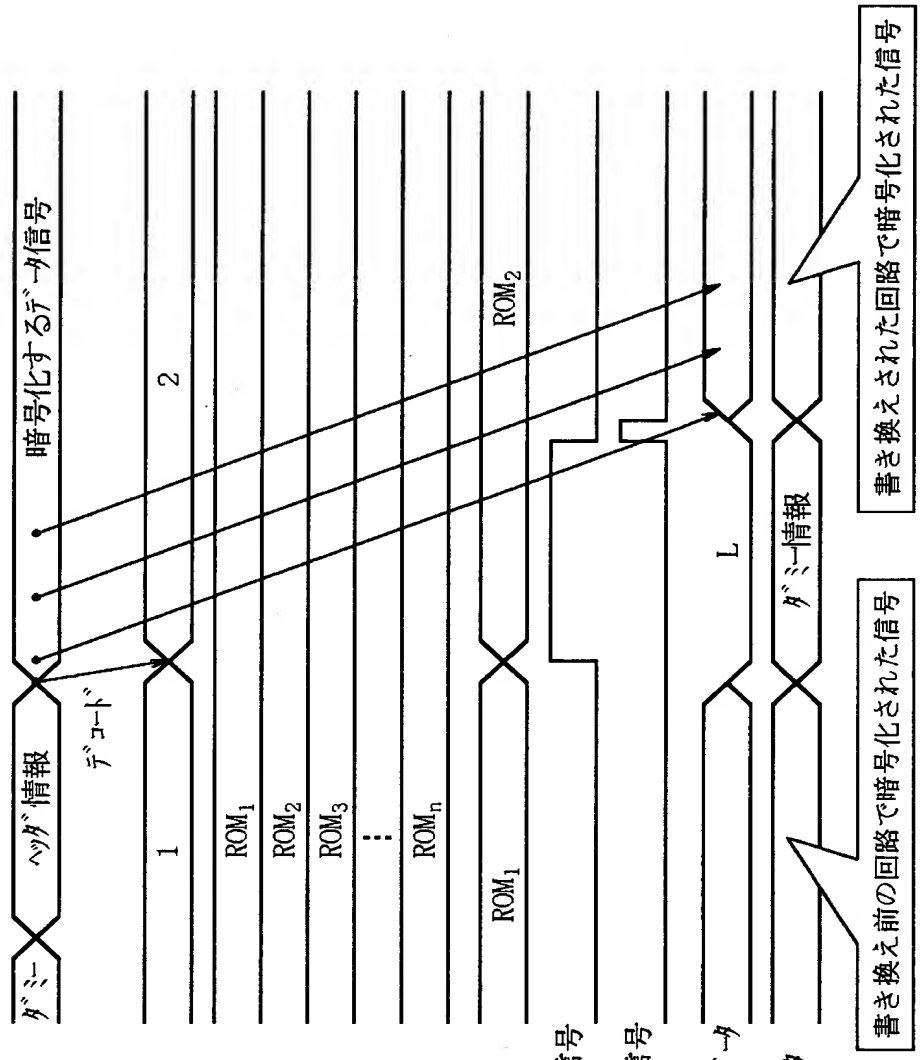
【図１】


102 送信装置
106 受信装置
103
107
110 暗号化ﾃﾞｰﾀ
可変処理回路
ﾈｯﾄﾜｰｸ網
可変処理回路
101 入力ﾃﾞｰﾀ
105 回路ﾃﾞｰﾀ (秘密鍵)
104
111
113 暗号化ﾃﾞｰﾀ
108
109 回路ﾃﾞｰﾀ (秘密鍵)
112 出力ﾃﾞｰﾀ
ROM
ROM

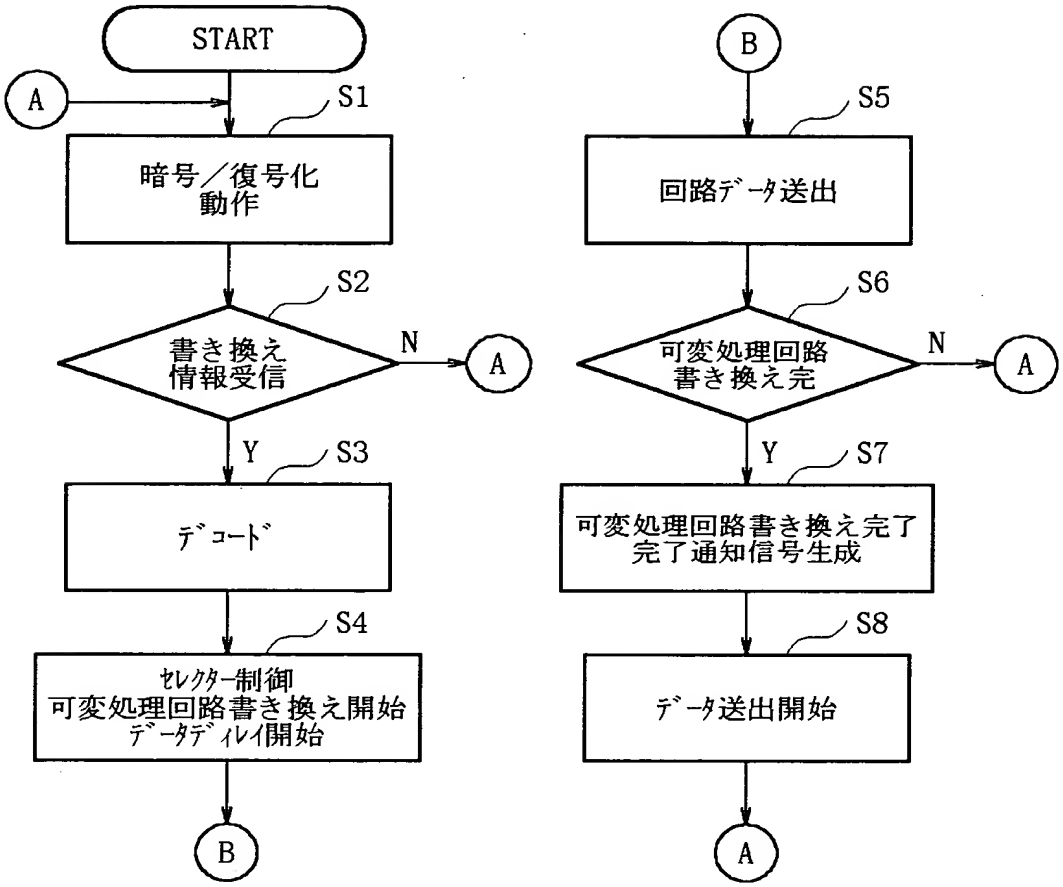
【図２】


201 送信装置
暗号／復号化データ保持部
204
209 終了通知信号
203
207
210 入力保持データ
データ解析部
可変処理回路
211 暗号化データ
202 入力データ
216
208 回路データ
205
セレクター
206
206a
206b
206n
ROM
ROM
ROM
ROM
111
ネットワーク網
201a 受信装置
暗号／復号化データ保持部
204a
209a 終了通知信号
203a
207a
210a 入力保持データ
データ解析部
可変処理回路
214 出力データ
213 暗号化データ
216a
208a 回路データ
205a
セレクター
215
215a
215b
215n
ROM
ROM
ROM
ROM

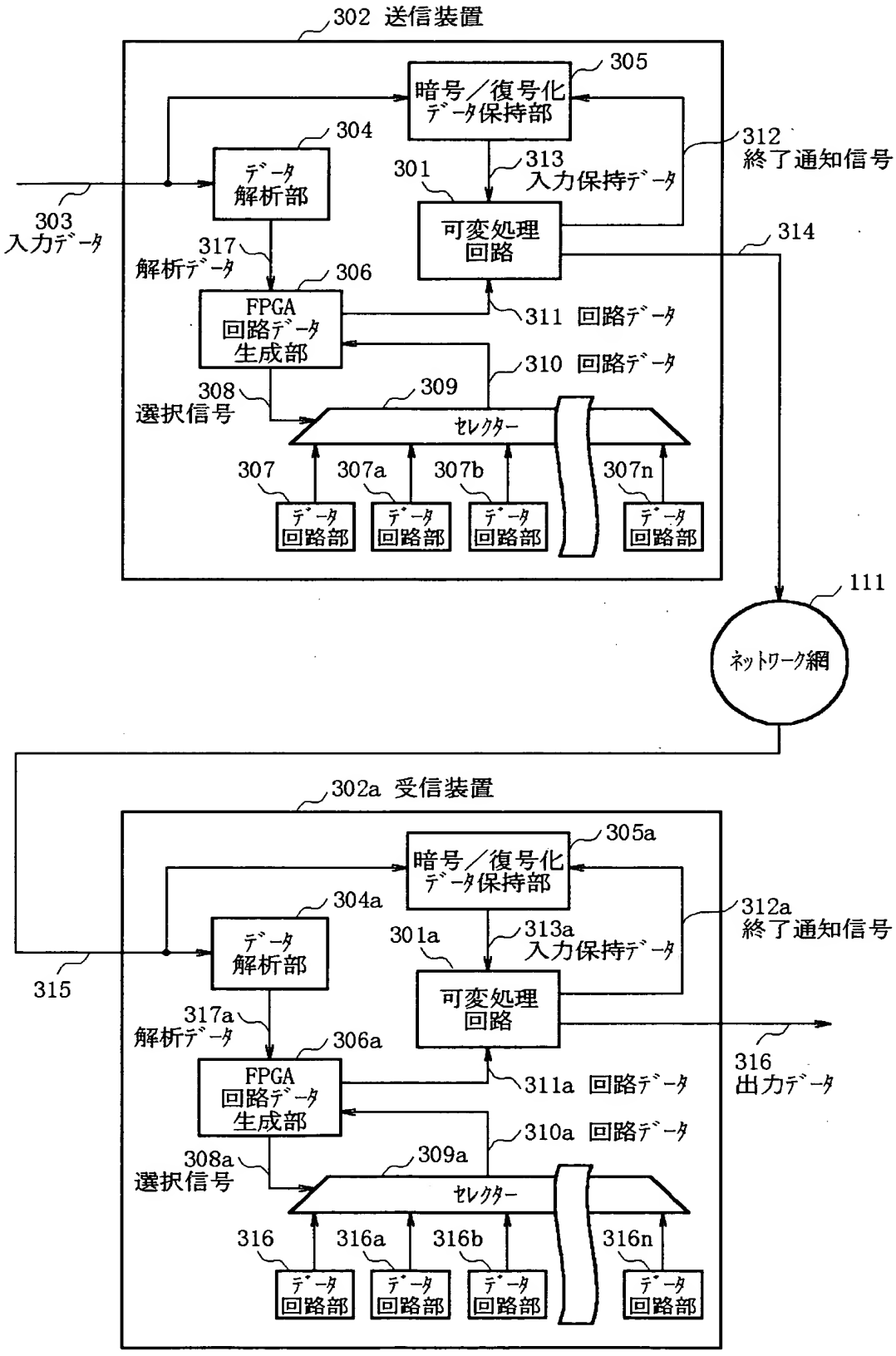
【図３】


202 入力
ﾀﾞﾐｰ
ﾍｯﾀﾞ情報
暗号化するﾃﾞｰﾀ信号
ﾃﾞｺｰﾄﾞ
205 ｾﾚｸﾀｰ
1
2
206 ROMの出力
ROM1
206a ROMの出力
ROM2
206b ROMの出力
ROM3
206n ROMの出力
ROMn
208 回路ﾃﾞｰﾀ
ROM1
ROM2
可変処理回路207の書き換え信号
209 終了通知信号
210 入力保持ﾃﾞｰﾀ
L
211 暗号化ﾃﾞｰﾀ
ﾀﾞﾐｰ情報
書き換え前の回路で暗号化された信号
書き換えされた回路で暗号化された信号

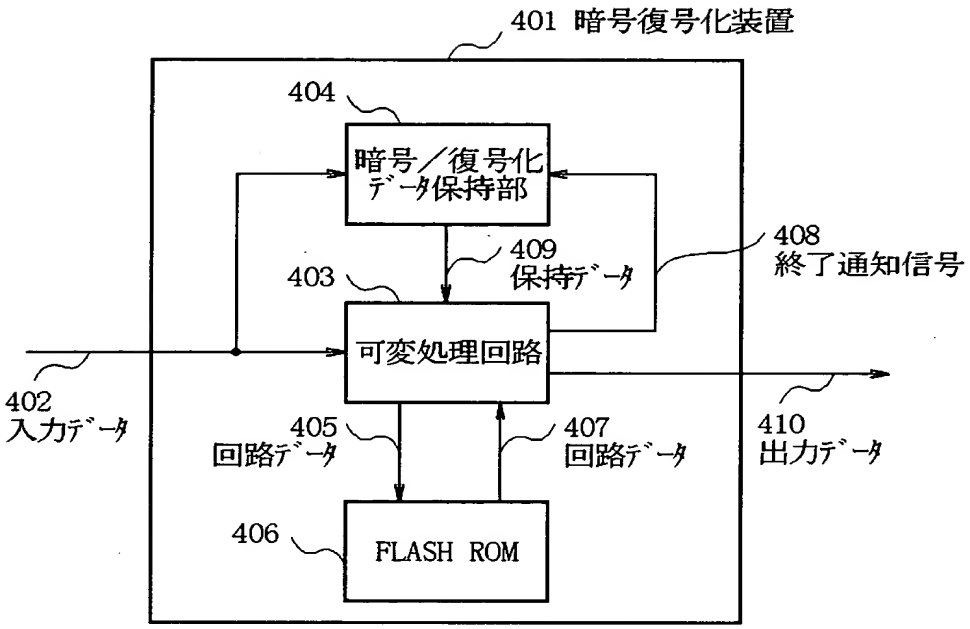
【図４】


START
A
S1
暗号／復号化
動作
S2
書き換え
情報受信
N
A
Y
S3
ﾃﾞｺｰﾄﾞ
S4
ｾﾚｸﾀｰ制御
可変処理回路書き換え開始
ﾃﾞｰﾀﾃﾞｨﾚｲ開始
B
B
S5
回路ﾃﾞｰﾀ送出
S6
可変処理回路
書き換え完
N
A
Y
S7
可変処理回路書き換え完了
完了通知信号生成
S8
ﾃﾞｰﾀ送出開始
A

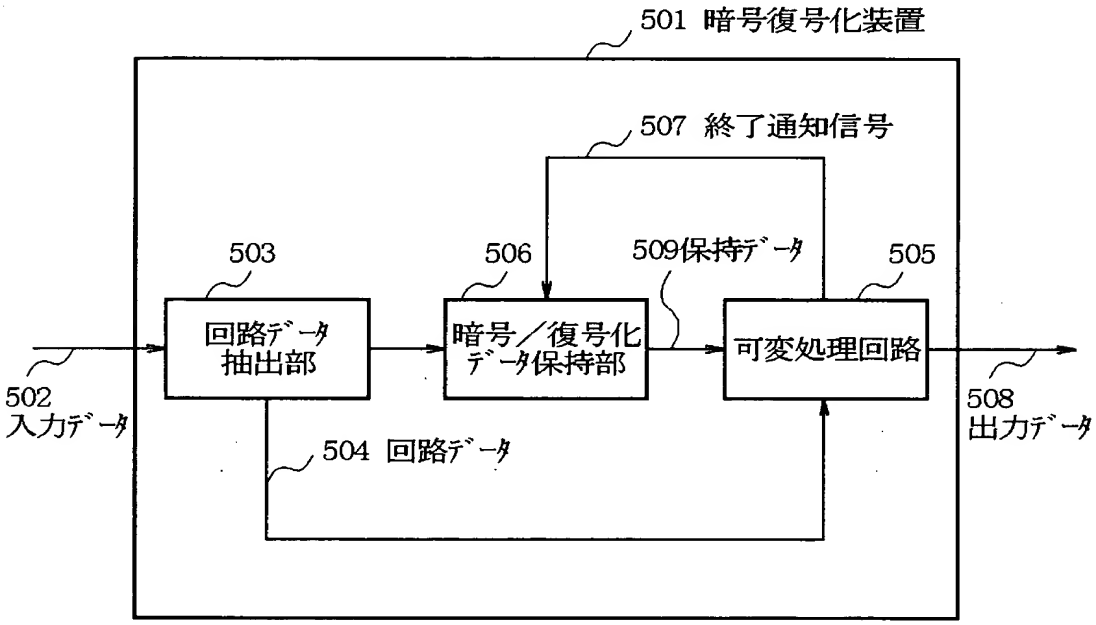
【図５】


302 送信装置
暗号／復号化データ保持部
305
304
データ解析部
312
終了通知信号
313
入力保持データ
301
303
入力データ
可変処理回路
314
317
解析データ
306
FPGA回路データ生成部
311 回路データ
310 回路データ
308
選択信号
309
セレクター
307
307a
307b
307n
データ回路部
111
ネットワーク網
302a 受信装置
暗号／復号化データ保持部
305a
304a
データ解析部
312a
終了通知信号
313a
入力保持データ
301a
315
可変処理回路
317a
解析データ
306a
316
出力データ
FPGA回路データ生成部
311a 回路データ
310a 回路データ
308a
選択信号
309a
セレクター
316
316a
316b
316n
データ回路部

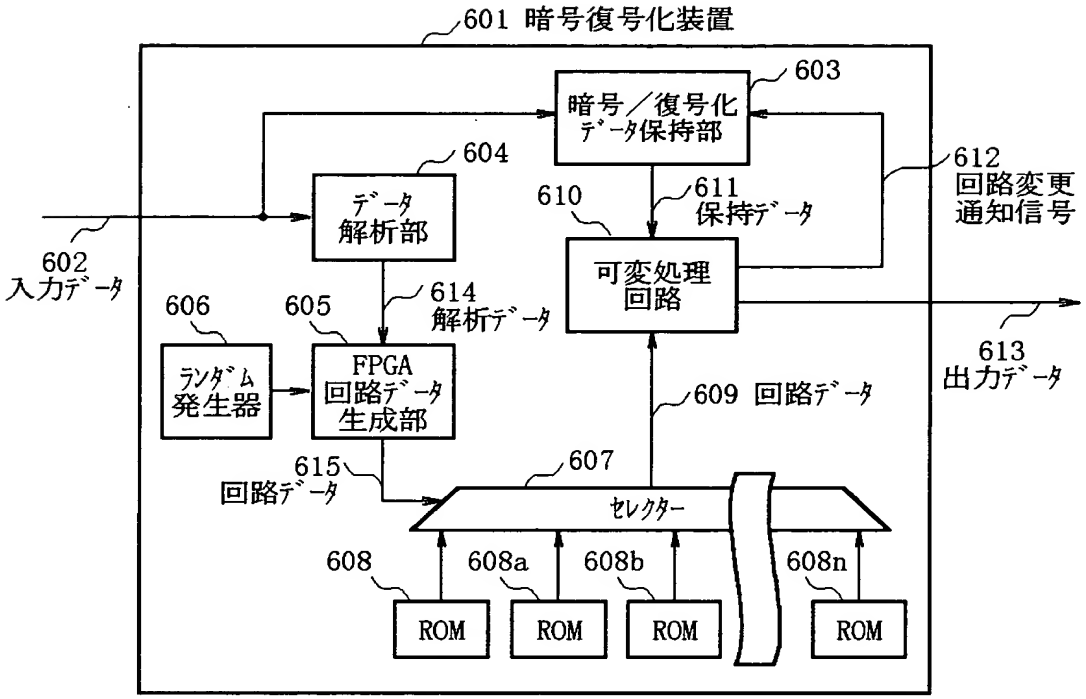
【図６】


401 暗号復号化装置
404
暗号／復号化
データ保持部
409
保持データ
408
終了通知信号
403
可変処理回路
402
入力データ
405
回路データ
407
回路データ
410
出力データ
406
FLASH ROM

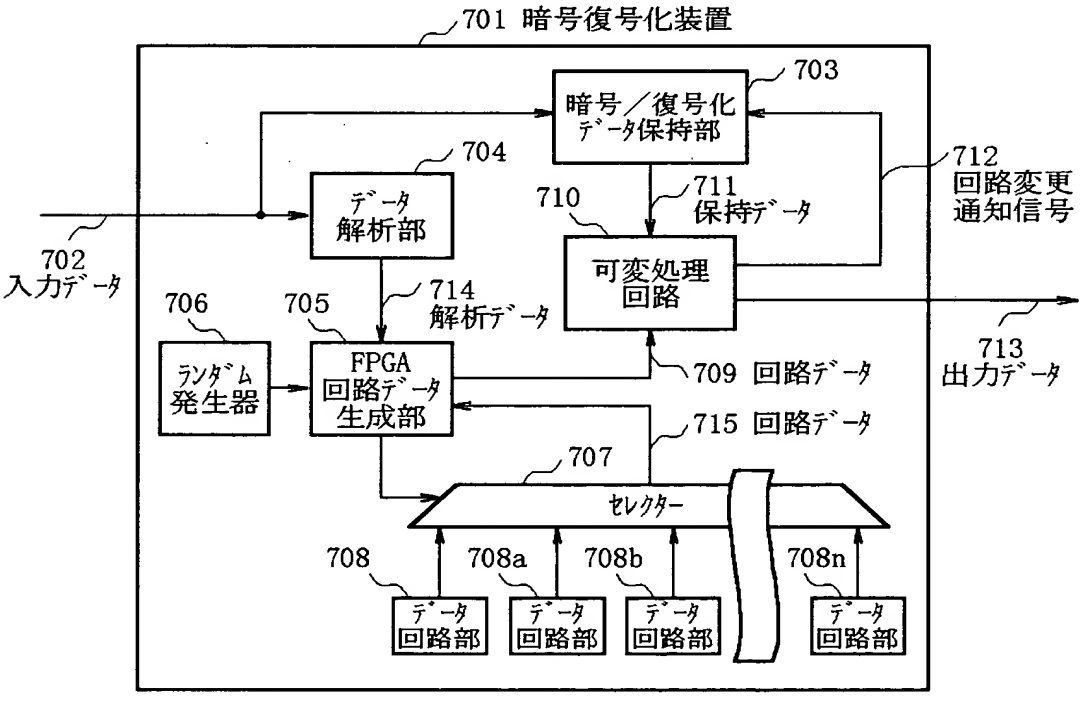
【図７】


501 暗号復号化装置
507 終了通知信号
503
506
509保持データ
505
回路データ
抽出部
暗号／復号化
データ保持部
可変処理回路
502
入力データ
508
出力データ
504 回路データ

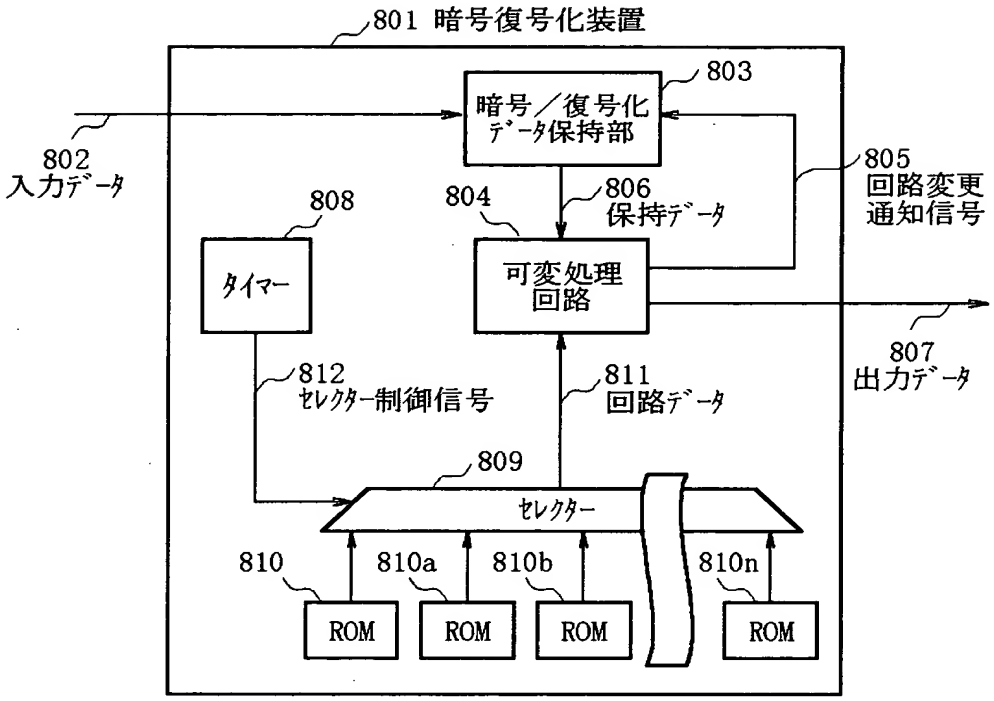
【図８】


601 暗号復号化装置
暗号／復号化
ﾃﾞｰﾀ保持部
603
604
ﾃﾞｰﾀ
解析部
610
611
保持ﾃﾞｰﾀ
612
回路変更
通知信号
602
入力ﾃﾞｰﾀ
可変処理
回路
606
605
614
解析ﾃﾞｰﾀ
ﾗﾝﾀﾞﾑ
発生器
FPGA
回路ﾃﾞｰﾀ
生成部
613
出力ﾃﾞｰﾀ
609 回路ﾃﾞｰﾀ
615
回路ﾃﾞｰﾀ
607
ｾﾚｸﾀｰ
608
608a
608b
608n
ROM
ROM
ROM
ROM

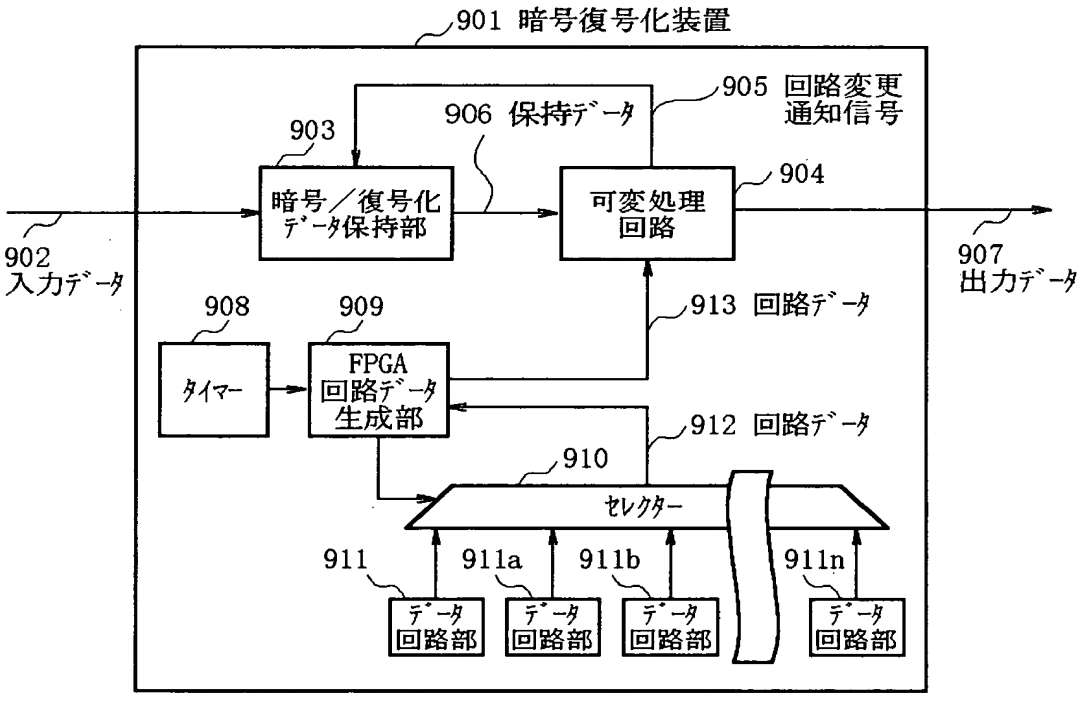
【図９】


701 暗号復号化装置
暗号／復号化
ﾃﾞｰﾀ保持部
703
704
ﾃﾞｰﾀ
解析部
710
711
保持ﾃﾞｰﾀ
712
回路変更
通知信号
702
入力ﾃﾞｰﾀ
可変処理
回路
706
705
714
解析ﾃﾞｰﾀ
ﾗﾝﾀﾞﾑ
発生器
FPGA
回路ﾃﾞｰﾀ
生成部
713
出力ﾃﾞｰﾀ
709 回路ﾃﾞｰﾀ
715 回路ﾃﾞｰﾀ
707
ｾﾚｸﾀｰ
708
708a
708b
708n
ﾃﾞｰﾀ
回路部
ﾃﾞｰﾀ
回路部
ﾃﾞｰﾀ
回路部
ﾃﾞｰﾀ
回路部

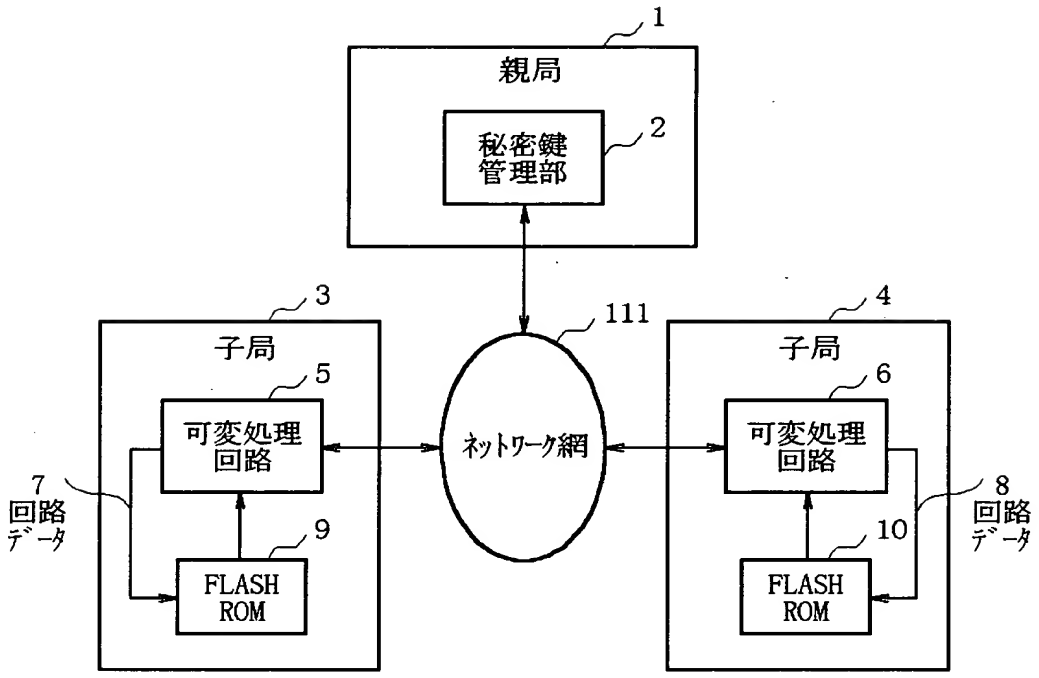
【図１０】


801 暗号復号化装置
803
暗号／復号化
ﾃﾞｰﾀ保持部
802
入力ﾃﾞｰﾀ
805
回路変更
通知信号
808
804
806
保持ﾃﾞｰﾀ
タイマー
可変処理
回路
807
出力ﾃﾞｰﾀ
812
ｾﾚｸﾀｰ制御信号
811
回路ﾃﾞｰﾀ
809
ｾﾚｸﾀｰ
810
810a
810b
810n
ROM
ROM
ROM
ROM

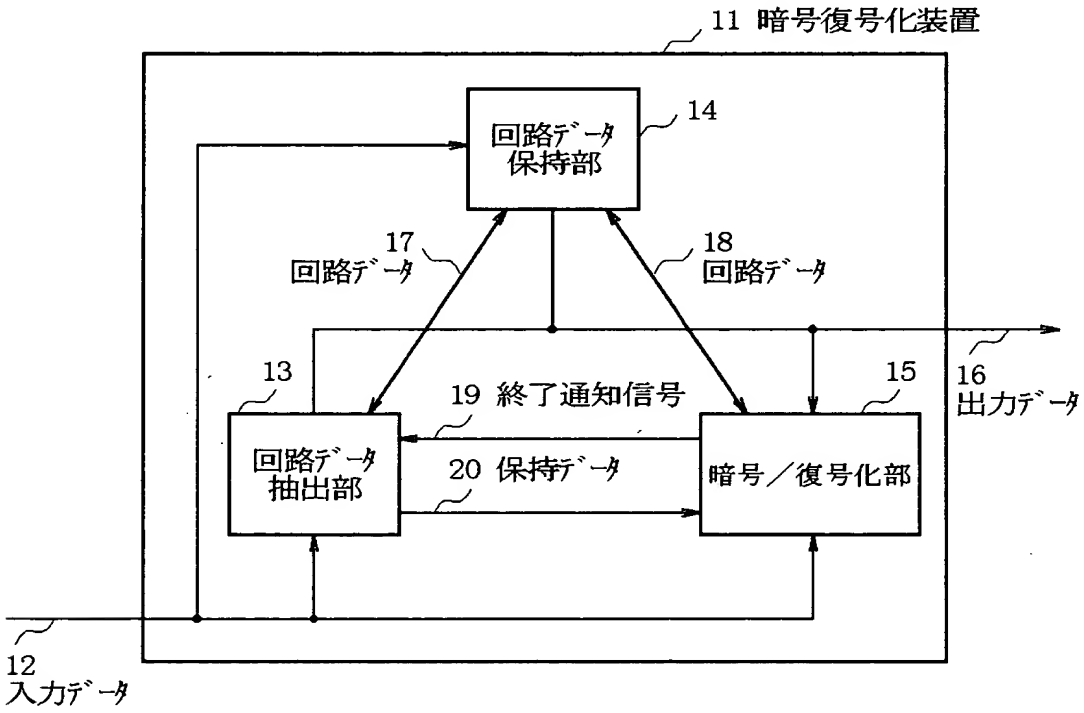
【図１１】


901 暗号復号化装置
905 回路変更
通知信号
903
906 保持ﾃﾞｰﾀ
904
暗号／復号化
ﾃﾞｰﾀ保持部
可変処理
回路
902
入力ﾃﾞｰﾀ
907
出力ﾃﾞｰﾀ
908
909
913 回路ﾃﾞｰﾀ
タイマー
FPGA
回路ﾃﾞｰﾀ
生成部
912 回路ﾃﾞｰﾀ
910
ｾﾚｸﾀｰ
911
911a
911b
911n
ﾃﾞｰﾀ
回路部
ﾃﾞｰﾀ
回路部
ﾃﾞｰﾀ
回路部
ﾃﾞｰﾀ
回路部

【図１２】


1
親局
秘密鍵
管理部
2
3
子局
5
可変処理
回路
7
回路
データ
9
FLASH
ROM
111
ネットワーク網
4
子局
6
可変処理
回路
8
回路
データ
10
FLASH
ROM

【図１３】


11 暗号復号化装置
回路データ
保持部
14
17
回路データ
18
回路データ
13
19 終了通知信号
15
16
出力データ
回路データ
抽出部
20 保持データ
暗号／復号化部
12
入力データ

【書類名】　　要約書

【要約】

【課題】暗号復号化方法のアルゴリズム変更に伴うハードウェア変更を可能とし、暗号復号の高速処理を図る。

【解決手段】送信装置１０２は入力データ１０１を暗号化し暗号化データ１１０を出力する。ネットワーク網１１１は暗号化データ１１０を伝送する。受信装置１０６はネットワーク網１１１を介して伝送されてきて暗号化データ１１３を入力し、暗号解読を行い復号化した出力データ１１２を出力する。

可変処理回路１０３は入力データ１０１暗号化する。ＲＯＭ１０４は秘密鍵の回路データ１０５を可変処理回路１０３に出力する。可変処理回路１０７は暗号化データ１１３を復号する。ＲＯＭ１０８は秘密鍵の回路データ１０９を可変処理回路１０７に出力する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－１１８２６９
受付番号	５００００４９５３１４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　４月２０日

＜認定情報・付加情報＞

【提出日】　平成12年 4月19日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００２３２２５４〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都港区三田１丁目４番２８号
氏　名　日本電気通信システム株式会社